03/8043-SNY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-102471

(43)Date of publication of application : 13.04.1999

(51)Int.Cl. G07F 7/08
G06K 17/00
G09C 1/00

(21)Application number : 09-262489

(22)Date of filing : 26.09.1997

(71)Applicant : NTT DATA CORP

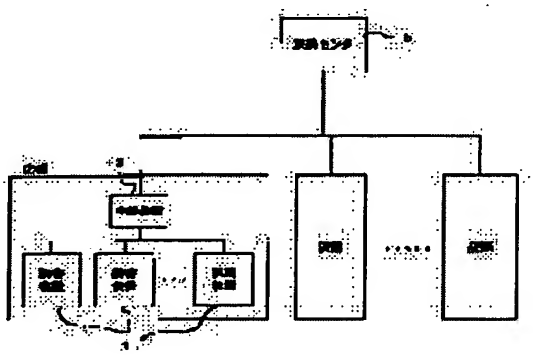
(72)Inventor : KUROI TOSHIO
KAMATA TAKAYUKI

(54) PREPAID CARD SYSTEM, CERTIFICATION SYSTEM, READER, MANAGEMENT DEVICE, AND DEVICE CERTIFICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a prepaid card system which can simultaneously transmit certification data to the device to be certified from a certification device, certifies them at a high speed, combines the ciphering of entire certification data and the ciphering of a part of data and discriminates the cause of the certification error of the device of the certification object.

SOLUTION: A relay device 3 designates a global address and simultaneously transmits all certification data to all readers 1. The respective readers 1 receiving certification data cipher a part of certification data with an individual password key, cipher the entire certification data with a common password and return them to the relay device 3. The relay device 3 decodes certification data returned from the readers 1 for certifying them commonly in the system and compares it with certification data. The relay device 3 compares a part of data certified by the readers 1 with the individual password in certification data returned from the readers 1 in certification data returned form the readers 1, with the password with a block which is the object of password data for certification for individually certifying the devices.



LEGAL STATUS

[Date of request for examination] 02.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－102471

(43)公開日　平成11年(1999)４月13日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０７Ｆ　7/08		Ｇ０７Ｆ　7/08	Ｊ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ
			Ｌ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｆ
			６６０Ｂ

審査請求　未請求　請求項の数19　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平9－262489

(22)出願日　平成９年(1997)９月26日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　黒井　俊夫
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　鎌田　隆之
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

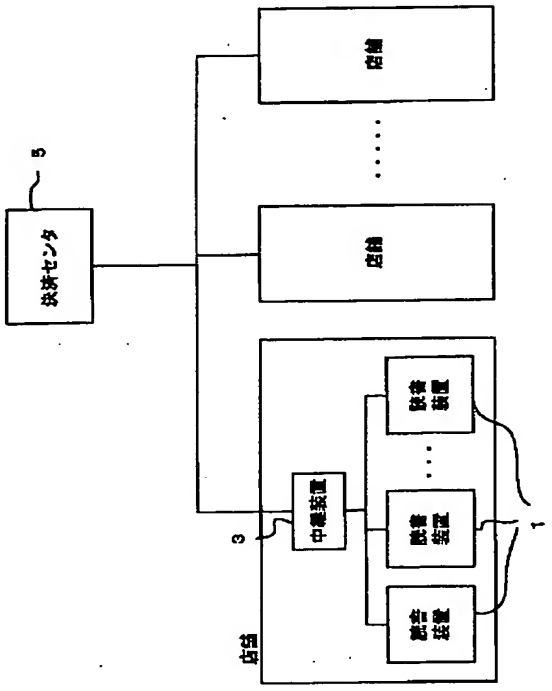
(74)代理人　弁理士　木村　満

(54)【発明の名称】　プリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法

(57)【要約】

【課題】　認証装置から認証対象装置に認証データを一斉に送信して高速に認証し、且つ、認証データ全体の暗号化と一部分のデータの暗号化とを組み合わせて、認証対象装置の認証ミスの原因を判別するプリペイドカードシステムを提供する。

【解決手段】　中継装置３は、グローバルアドレスを指定して認証データを全ての読書装置１に一斉に送信する。認証データを受信した各読書装置１は、認証データの一部分を個別暗号鍵ｋｅｉで暗号化し、さらに共通暗号鍵ｋｆで認証データ全体を暗号化し、中継装置３に返送する。中継装置３は、読書装置１から返送された認証データを、システムで共通に認証するため、共通暗号鍵ｋｆで復号化して、検証データと比較する。次に、中継装置３は、装置を個別に認証するため、読書装置１から返送された認証データのうち読書装置１が個別暗号鍵ｋｅｉで暗号化した一部分と検証用暗号データの対象となるブロックとを比較する。



【特許請求の範囲】

【請求項１】金額情報を有するプリペイドカードを処理するための複数の読書装置と、複数の前記読書装置を管理する中継装置と、各店舗の前記中継装置と通信により接続された決済センタと、を備えるプリペイドカードシステムにおいて、

前記読書装置は、前記中継装置から送信されて来た認証データを暗号化して前記中継装置に返送し、

前記中継装置は、複数の前記読書装置に認証データを一斉に送信し、返送された各認証データから各前記読書装置を認証し、前記認証データから前記読書装置を認証できない場合に、認証できない読書装置を特定する情報と共に異常情報を前記決済センタに送信し、

前記決済センタは、前記中継装置から送信された異常情報から異常な読書装置を特定する、

ことを特徴とするプリペイドカードシステム。

【請求項２】前記読書装置は、前記中継装置から送信されて来た認証データの一部を暗号化して前記中継装置に返送し、

前記中継装置は、返送された、一部が暗号化された認証データから各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシステム。

【請求項３】前記読書装置は、前記中継装置から送信されて来た認証データの一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、複数の読書装置に共通の共通暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、返送されて来た認証データが前記共通暗号化方式で暗号化され、且つ、その一部が前記個別暗号化方式で暗号化されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシステム。

【請求項４】前記中継装置は、検証データを前記複数の読書装置に共通の第１の共通暗号化方式で暗号化して認証データを生成して各読書装置に送信し、

前記読書装置は、前記中継装置から送信されて来た認証データを前記第１の共通暗号化方式に従って復号化した後、その一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、前記複数の読書装置に共通の第２の共通暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、返送されて来た認証データが前記第１及び第２の共通暗号化方式で適切に処理されているか否か、及び、その一部が前記個別暗号化方式で適切に暗号化されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシステム。

【請求項５】前記中継装置にはｎ（ｎは２以上の自然数）台の前記読書装置が接続され、

前記認証データはｎ個のデータブロックを含み、

前記ｎ台の読書装置のうち、第ｉ（ｉはｎ以下の自然数）の読書装置は、前記中継装置から送信されて来た認証データのうちの、第ｉのデータブロックのデータを自己に割り当てられた個別暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、前記第ｉの読書装置から返送されて来た認証データの第ｉのデータブロックのデータが、各読書装置に送信した認証データの第ｉのデータブロックに実質的に一致するか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシステム。

【請求項６】前記中継装置にはｎ（ｎは２以上の自然数）台の前記読書装置が接続され、

前記ｎ台の読書装置のうち、第ｉ（ｉはｎ以下の自然数）の読書装置は、前記中継装置から受信した認証データの第ｉのブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、前記第ｉのブロックのデータが暗号化された認証データを前記共通暗号鍵で暗号化して前記中継装置に返送し、

前記中継装置は、前記第ｉの読書装置から返送されて来た認証データの第ｉのブロック以外の領域が前記共通暗号鍵により処理されているか否かを判別することと、前記第ｉのブロックが前記個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシステム。

【請求項７】前記中継装置にはｎ（ｎは２以上の自然数）台の前記読書装置が接続され、

前記中継装置は、ｎ個のデータブロックを含む検証データを第１の共通暗号鍵で暗号化して認証データを生成し、

前記ｎ台の読書装置のうち、第ｉ（ｉはｎ以下の自然数）の読書装置は、前記中継装置から受信した認証データを前記第１の共通暗号鍵で復号し、復号した認証データの第ｉのブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、前記第ｉのブロックのデータが暗号化された認証データを第２の共通暗号鍵で暗号化して前記中継装置に返送し、

前記中継装置は、前記第ｉの読書装置から返送されて来た認証データの第ｉのブロック以外の領域が前記第２の共通暗号鍵により処理されているか否かを判別することと、前記第ｉのブロックが前記個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項１に記載のプリペイドカードシ

ステム。
【請求項８】前記中継装置は、
前記第ｉの読書装置から返送されて来た認証データの第ｉのブロック以外の領域が前記第２の共通暗号鍵により処理されているか否かを判別することにより、前記第ｉの読書装置がこのプリペイドカードシステムに使用可能な装置であるか否かを判別し、
前記第ｉのブロックが前記個別暗号鍵により処理されているか否かを判別することにより、前記読書装置の設定のエラーの有無を判別する、
ことを特徴とする請求項７に記載のプリペイドカードシステム。
【請求項９】ｎ台の被認証装置と、前記ｎ台の被認証装置を管理する認証装置と、を備えるシステムにおいて、
前記認証装置は、ｎ個のデータブロックを含む認証データを、前記ｎ台の被認証装置に送信し、
前記ｎ台の被認証装置のうち、第ｉ（ｉはｎ以下の自然数）の被認証装置は、前記認証装置から送信されて来た認証データの第ｉのブロックのデータを個別の暗号鍵ｋｅｉで暗号化して前記認証装置に返送し、
前記認証装置は、前記第ｉの被認証装置から返送されて来た認証データの第ｉのブロックのデータが期待値に実質的に一致するか否かを判別することにより、各前記被認証装置を認証する、
ことを特徴とする認証システム。
【請求項１０】前記第ｉ（ｉはｎ以下の自然数）の被認証装置は、前記認証装置から送信されて来た認証データの第ｉのブロックのデータを個別の暗号鍵ｋｅｉで暗号化し、前記第ｉのブロックのデータが暗号化された認証データを前記複数の被認証装置に共通の暗号鍵ｋｆで暗号化して前記認証装置に返送し、
前記認証装置は、前記第ｉの被認証装置から返送されて来た認証データの第ｉのブロック以外のブロックのデータが期待値に実質的に一致するか否かを判別すること、及び、前記第ｉの被認証装置から返送されて来た認証データの第ｉのブロックのデータが期待値に実質的に一致するか否かを判別することにより、各前記被認証装置を認証する、
ことを特徴とする請求項９に記載の認証システム。
【請求項１１】プリペイドカードを処理するための読書装置であって、
認証データを受信する手段と、前記受信手段で受信した認証データを暗号鍵ｋｆ１で復号化する復号化手段と、前記復号化手段により復号化された認証データ中の所定の一部のデータを暗号鍵ｋｅｉで暗号化し、さらに、一部が暗号化された認証データを暗号鍵ｋｆ２で暗号化して出力する手段と、
を備えることを特徴とする読書装置。
【請求項１２】前記暗号鍵ｋｆ１と前記暗号鍵ｋｆ２は、実質的に等しい、
ことを特徴とする請求項１１に記載の読書装置。
【請求項１３】プリペイドカードを処理するための読書装置を認証して管理する上位装置であって、
認証データを複数の読書装置に一斉に送信する送信手段と、
各読書装置から送信されて来た認証データを受信する受信手段と、
前記受信手段で受信した認証データに基づいて各読書装置を認証する認証手段と、
を備えることを特徴とする管理装置。
【請求項１４】前記認証手段は、前記受信手段で受信した認証データが期待値に実質的に一致するか否かを判別することにより、認証を行う、ことを特徴とする請求項１３に記載の管理装置。
【請求項１５】前記送信手段は、検証データを複数の読書装置に共通の暗号鍵ｋｆで暗号化して認証データを生成して前記複数の読書装置に送信し、
前記認証手段は、前記受信手段で受信した認証データを前記暗号鍵ｋｆで復号化し、復号化したデータが実質的に期待値に一致するか否かに基づいて各読書装置を認証する、
ことを特徴とする請求項１４に記載の管理装置。
【請求項１６】前記認証手段は、前記受信手段で受信した認証データを前記暗号鍵ｋｆで復号化し、前記暗号鍵ｋｆで復号化した認証データの、各読書装置に割り付けられた一部が前記検証データに実質的に一致するか否かに基づいて各読書装置を認証する、
ことを特徴とする請求項１５に記載の管理装置。
【請求項１７】プリペイドカードから得た金額情報を取り扱う装置を認証する方法であって、
認証データを一度に複数の認証相手装置に送信する一斉送信ステップと、
前記一斉送信ステップで送信された認証データを受信し、受信した認証データを暗号鍵で暗号化し、暗号化した認証データを返送する認証データ更新ステップと、
前記認証データ更新ステップから返送された認証データを受信する受信ステップと、
前記受信ステップが受信した認証データと認証相手装置を認証することのできる検証データとを比較して認証相手装置を認証する認証ステップと、
を備えることを特徴とする装置認証方法。
【請求項１８】同一の認証データを複数の相手装置に一斉送信し、
各相手装置が、受信した認証データのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを返送し、
返送された認証データを受信し、
受信した認証データと前記検証データとを比較して認証相手装置を認証する、
ことを特徴とする装置認証方法。

【請求項１９】同一の認証データを複数の認証相手装置に送信する際に、該複数の認証相手装置に共通の暗号化方式で暗号化して一斉送信し、
各相手装置が、受信した認証データを復号化した後、復号化したデータのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを共通の暗号化方式で暗号化して返送し、
返送された認証データを受信し、
受信した認証データと前記検証データとを比較して認証相手装置を認証する、
ことを特徴とする装置認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信による装置の認証を高速化することのできるプリペイドカードシステム、認証システム、読書装置及び装置認証方法に関する。

【０００２】

【従来の技術】従来のプリペイドカードシステムにおいて、プリペイドカードに記憶されている金額情報を使用するための読書装置は、使用された金額情報等をセンタ等の上位装置に送信する。上位装置は、このような金額情報等が、売上金となる重要なデータであるため、セキュリティ上、正当なデータであり、しかも正しい相手からのデータであることを確認する必要がある。

【０００３】上位装置は、読書装置が正しい相手であることを確認するために、通信により装置の認証を行う。通信による装置の認証を、例えば、秘密鍵暗号方式の場合について説明すると、まず、認証側の装置となる上位装置は、平文のデータＡを相手装置となる読書装置に送信する。読書装置は、受信したデータＡを、記憶している暗号鍵ｋｅを使用して暗号化し、データＡ’とする。読書装置は、暗号化したデータＡ’を上位装置に返送する。上位装置は、読書装置から返送されたデータＡ’と、読書装置に送信した平文のデータＡを自ら記憶している暗号鍵ｋｅを使用して暗号化しておいたデータＡ’とを比較する。上位装置は、互いの暗号鍵ｋｅを使用して暗号化された２つのデータＡ’が一致すると判別した場合に、読書装置が正しい相手であることを認証する。また、上位装置が、多数の読書装置を認証する場合には、認証相手である読書装置毎に異なる暗号鍵を認証に使用して、データ改竄や偽造装置からの偽造データの発生に対する安全性を高めている。

【０００４】

【発明が解決しようとする課題】しかし、大規模なプリペイドカードシステムともなると、読書装置が多数設置されているため、全ての読書装置を個別に認証すると、装置認証による負荷が大きくなる。このため、一般的に、公開鍵暗号方式よりも比較的処理を高速に行える秘密鍵暗号方式を認証に用いるなどの対策をしても、認証に必要なデータの送受信に時間がかかるため、認証を高速化することが困難であった。

【０００５】また、読書装置ごとに異なる暗号鍵を認証に使用する場合では、暗号鍵の配付の誤りや読書装置の設置の誤り等、設定上の誤りが発生する割合が高くなる。従って、読書装置の認証できなかった場合でも、データ改竄や偽造装置が原因と断定する前に、設定の確認が必要となり、迅速な対処をすることが困難となっていた。

【０００６】本発明は、上記実状に鑑みてなされたもので、通信による読書装置の認証を高速化することができるプリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法を提供することを目的とする。また、本発明は、設定上の誤りを原因とする読書装置の認証不能を適切に判別することのできるプリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係るプリペイドカードシステムは、金額情報を有するプリペイドカードを処理するための複数の読書装置と、複数の前記読書装置を管理する中継装置と、各店舗の前記中継装置と通信により接続された決済センタと、を備えるプリペイドカードシステムにおいて、前記読書装置は、前記中継装置から送信されて来た認証データを暗号化して前記中継装置に返送し、前記中継装置は、複数の前記読書装置に認証データを一斉に送信し、返送された各認証データから各前記読書装置を認証し、前記認証データから前記読書装置を認証できない場合に、認証できない読書装置を特定する情報と共に異常情報を前記決済センタに送信し、前記決済センタは、前記中継装置から送信された異常情報から異常な読書装置を特定する、ことを特徴とする。

【０００８】このような構成によれば、中継装置から読書装置へ認証データの送信を一斉にすることで認証を高速化することができる。また、中継装置は、読書装置を認証できない場合に、異常情報を中継装置の上位装置である決済センタに送信する。決済センタは、受信した異常情報から該当する読書装置を特定することができる。従って、最上位装置である決済センタが最下位装置である読書装置の認証異常を把握することができる。

【０００９】読書装置は、中継装置から送信されて来た認証データの一部を暗号化して中継装置に返送し、中継装置は、返送された、一部が暗号化された認証データから各読書装置を認証してもよい。この構成によれば、中継装置は、一部が暗号化された認証データから、読書装置を認証する。従って、読書装置は、認証データの一部分のみを暗号化すればよく、結果として、システム全体の認証を高速化することができる。

【００１０】読書装置は、中継装置から送信されて来た

認証データの一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、認証データ全部を、各読書装置に共通の共通暗号化方式で暗号化して中継装置に返送し、中継装置は、返送されて来た認証データが共通暗号化方式で暗号化され、且つ、その一部が個別暗号化方式で暗号化されているか否かを判別することにより、各読書装置を認証してもよい。

【００１１】この構成によれば、中継装置は、共通暗号化方式による暗号化が不適切なために認証データを認証できない場合には、その装置自体に何らかの異常（偽物装置である可能性を含めて）があると推測できる。また、共通暗号化方式による暗号化は適切に行われているが、個別暗号化方式による暗号化が不適切なために認証データを認証できない場合には、読書装置の設定のミスなどが原因であると推測できる。従って、異常の原因の推測も可能である。

【００１２】また、中継装置は、検証データを複数の読書装置に共通の第１の共通暗号化方式で暗号化して認証データを生成して各読書装置に送信し、読書装置は、中継装置から送信されて来た認証データを第１の共通暗号化方式に従って復号化した後、その一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、複数の読書装置に共通の第２の共通暗号化方式で暗号化して中継装置に返送し、中継装置は、返送されて来た認証データが第１及び第２の共通暗号化方式で適切に処理されているか否か、及び、その一部が個別暗号化方式で適切に暗号化されているか否かを判別することにより、各前記読書装置を認証してもよい。

【００１３】この構成によれば、認証データが第１及び第２の共通暗号化方式で適切に処理されているか否かを判別することにより、読書装置の異常を推測することができる。また、認証データが第１及び第２の共通暗号化方式で適切に処理されているが、個別暗号化方式で適切に処理されていない場合には、読書装置の設定や配置のミスであることが推測できる。従って、異常の原因の推測も可能である。

【００１４】例えば、中継装置には、ｎ（ｎは２以上の自然数）台の読書装置が接続され、認証データはｎ個のデータブロックを含み、ｎ台の読書装置のうち、第ｉ（ｉはｎ以下の自然数）の読書装置は、中継装置から送信されて来た認証データのうちの、第ｉのデータブロックのデータを自己に割り当てられた個別暗号化方式で暗号化して中継装置に返送し、中継装置は、第ｉの読書装置から返送されて来た認証データの第ｉのデータブロックのデータが、各読書装置に送信した認証データの第ｉのデータブロックに実質的に一致するか否かを判別することにより、各前記読書装置を認証してもよい。

【００１５】この構成によれば、複数の読書装置に同一の認証データを送信しながら、読書装置を個別に認証することができる。

【００１６】第ｉの読書装置は、中継装置から受信した認証データの第ｉのブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、認証データ全体を共通暗号鍵で暗号化して中継装置に返送し、中継装置は、第ｉの読書装置から返送されて来た認証データの第ｉのブロック以外の領域が共通暗号鍵により処理されているか否かを判別することと、第ｉのブロックが個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証してもよい。

【００１７】この構成によれば、中継装置は、読書装置が共通暗号鍵と個別暗号鍵とを適切に使用できるか否かにより認証することができる。しかも、共通暗号鍵を適切に使用できるか否かにより、このプリペイドカードシステムで使用できる読書装置であるか否かを推測することができ、個別暗号鍵を適切に使用できるか否かにより、読書装置の設定などのミスの有無等を推測できる。即ち、異常の原因を推測することも可能である。

【００１８】また、中継装置が、認証データを共通暗号鍵で暗号化してから、各読書装置に送信し、各読書装置が受信した認証データを復号してから、上述の処理を行うようにしてもよい。

【００１９】中継装置は、第ｉの読書装置から返送されて来た認証データの第ｉのブロック以外の領域が共通暗号鍵により処理されているか否かを判別ことにより、第ｉの読書装置がこのプリペイドカードシステムに使用可能な装置であるか否かを判別し、第ｉのブロックが個別暗号鍵により処理されているか否かを判別することにより、前記読書装置の設定のエラーの有無を判別することができる。

【００２０】中継装置は、第ｉの読書装置から返送された認証データを、第ｉのブロック以外の領域が共通暗号鍵により処理されているか否かと、第ｉのブロックが個別暗号鍵により処理されているか否かと、から第ｉの読書装置を認証する。従って、中継装置は、第ｉの読書装置を認証できない場合に、第ｉのブロック以外の領域と第ｉのブロックから認証できない原因を判別することができる。

【００２１】また、この発明の第２の観点に係る認証システムは、ｎ台の被認証装置と、前記ｎ台の被認証装置を管理する認証装置と、を備えるシステムにおいて、前記認証装置は、ｎ個のデータブロックを含む認証データを、前記ｎ台の被認証装置に送信し、前記ｎ台の被認証装置のうち、第ｉ（ｉはｎ以下の自然数）の被認証装置は、前記認証装置から送信されて来た認証データの第ｉのブロックのデータを個別の暗号鍵ｋｅｉで暗号化して前記認証装置に返送し、前記認証装置は、前記第ｉの被認証装置から返送されて来た認証データの第ｉのブロックのデータが期待値に実質的に一致するか否かを判別することにより、各読書装置を認証する。

【００２２】この構成によれば、認証装置から一度に複数の被認証装置に同一の認証データを送って、各被認証装置の認証処理が可能となる。

【００２３】第ｉの被認証装置は、認証装置から送信されて来た認証データの第ｉのブロックのデータを個別の暗号鍵ｋｅｉで暗号化し、第ｉのブロックのデータが暗号化された認証データを複数の被認証装置に共通の暗号鍵ｋｆで暗号化して認証装置に返送し、認証装置は、第ｉの被認証装置から返送されて来た認証データの第ｉのブロック以外のブロックのデータが期待値に実質的に一致するか否かと、第ｉの被認証装置から返送されて来た認証データの第ｉのブロックのデータが期待値に実質的に一致するか否かとを判別することにより、各被認証装置を認証してもよい。

【００２４】この構成によれば、共通暗号鍵ｋｆによる認証ができない場合には、被認証装置がシステム内で使用できない装置であることが推測できる。一方、個別暗号鍵ｋｅｆによる認証ができない場合には、被認証装置の配置や設定のミスであることが推測できる。

【００２５】また、この発明の第３の観点に係る読書装置は、プリペイドカードを処理するための読書装置であって、認証データを受信する手段と、前記受信手段で受信した認証データを暗号鍵ｋｆ１で復号化する復号化手段と、前記復号化手段により復号化された認証データの所定の一部のデータを暗号鍵ｋｅｉで暗号化し、さらに、認証データ全体を暗号鍵ｋｆ２で暗号化して出力する手段と、を備えることを特徴とする。

【００２６】このような構成によれば、読書装置は、認証データの一部を暗号鍵ｋｅｉで暗号化し、さらに、認証データ全体を暗号鍵ｋｆ２で暗号化して出力する。従って、読書装置からこのような認証データを返送された上位装置等は、読書装置を認証できない場合に、暗号鍵ｋｅｉで暗号化された認証データの一部と暗号鍵ｋｆ２で暗号化された認証データとから認証できない原因を判別することができる。

【００２７】暗号鍵ｋｆ１と暗号鍵ｋｆ２は、実質的に等しくてもよい。

【００２８】また、この発明の第４の観点に係る管理装置は、プリペイドカードを処理するための読書装置を認証して管理する上位装置であって、認証データを複数の読書装置に一斉に送信する送信手段と、各読書装置から送信されて来た認証データを受信する受信手段と、前記受信手段で受信した認証データに基づいて各読書装置を認証する認証手段と、を備えることを特徴とする。

【００２９】このような構成によれば、管理装置は、読書装置に認証データを一斉に送信し、各読書装置から返送された認証データを検証することにより、各読書装置の認証をすることができる。従って、中継装置から読書装置へ認証データの送信を一斉にすることで認証を高速化することができる。

【００３０】認証手段は、受信手段で受信した認証データが期待値に実質的に一致するか否かを判別することにより、認証を行ってもよい。

【００３１】送信手段は、検証データを複数の読書装置に共通の暗号鍵ｋｆで暗号化して認証データを生成して複数の読書装置に送信し、認証手段は、受信手段で受信した認証データを暗号鍵ｋｆで復号化し、復号化したデータが実質的に期待値に一致するか否かに基づいて認証してもよい。

【００３２】認証手段は、受信手段で受信した認証データを暗号鍵ｋｆで復号化し、暗号鍵ｋｆで復号化した認証データの、各読書装置に割り付けられた一部が前記検証データに実質的に一致するか否かに基づいて認証してもよい。

【００３３】また、この発明の第４の観点に係る装置認証方法は、プリペイドカードから得た金額情報を取り扱う装置を認証する方法であって、認証データを一度に複数の認証相手装置に送信する一斉送信ステップと、前記一斉送信ステップで送信された認証データを受信し、受信した認証データを暗号鍵で暗号化し、暗号化した認証データを返送する認証データ更新ステップと、前記認証データ更新ステップから返送された認証データを受信する受信ステップと、前記受信ステップが受信した認証データと認証相手装置を認証することのできる検証データとを比較して認証相手装置を認証する認証ステップと、を備える、ことを特徴とする。

【００３４】このような方法によれば、認証相手装置に認証データを一斉に送信し、各認証相手装置から返送された認証データを検証することにより、各認証相手装置の認証をすることができる。従って、認証相手装置へ認証データの送信を一斉にすることで認証を高速化することができる。

【００３５】同一の認証データを複数の相手装置に一斉送信し、各相手装置が、受信した認証データのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを返送し、返送された認証データを受信し、受信した認証データと検証データとを比較して認証相手装置を認証してもよい。

【００３６】一部が暗号化された認証データから認証データを暗号化した認証相手装置を認証する。従って、各認証相手装置の暗号化処理が速くなり、全体の認証を高速化することができる。

【００３７】同一の認証データを複数の認証相手装置に送信する際に、複数の認証相手装置に共通の暗号化方式で暗号化して一斉送信し、各相手装置が、受信した認証データを復号化した後、復号化したデータのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを共通の暗号化方式で暗号化して返送し、返送された認証データを受信し、受信した認証データと検証データとを比較して認証相手

装置を認証してもよい。

【００３８】認証相手装置が割り当てられた暗号鍵で一部を暗号化した認証データを受信し、受信した認証データと検証データを比較して認証相手装置を認証する。従って、認証相手装置を認証できない場合に、一部を暗号化された認証データから認証できない原因を判別することができる。

【００３９】

【発明の実施の形態】本発明の実施の形態にかかるプリペイドカードシステムについて以下図面を参照して説明する。このプリペイドカードシステムは、図１に示すように、各店舗に設置された読書装置１及び中継装置３と、決済センタ５と、を備える。

【００４０】読書装置１は、例えば、商品（サービス）の購入、貸出、提供等の対価の支払の場面において、プリペイドカードが記憶する金額情報を使用するための装置である。読書装置１は、各店舗に配置され、図２に示すように、カード読書部１１と、記憶部１３と、制御部１５と、通信制御部１７と、を備える。

【００４１】カード読書部１１は、装着されたプリペイドカードに記憶されているデータの読取り／書込みを行う。

【００４２】記憶部１３は、読書装置１で使用（消費）された決済金額情報を記憶する。また、記憶部１３は、上位装置となる中継装置３から認証のために認証データが送信された際に、認証データの更新処理に使用する共通暗号鍵ｋｆと個別暗号鍵ｋｅ（例えば、ＤＥＳ方式の秘密鍵等）を記憶する。共通暗号鍵ｋｆは、全ての読書装置１に共通の暗号鍵である。また、個別暗号鍵ｋｅは、読書装置１ごとに異なる暗号鍵である。さらに、記憶部１３は、自らを識別する装置ＩＤ（装置識別コード）を記憶する。

【００４３】制御部１５は、プリペイドカードの使用要求に応答し、使用金額に応じて、カード読書部１１に装着されているプリペイドカードの金額（残高）情報を更新すると共に、記憶部１３に記憶している決済金額情報に使用金額を加算する。また、制御部１５は、上位装置となる中継装置３から認証のために認証データが送信された際に、通信制御部１７を介して認証データを受信し、記憶部１３に記憶された共通暗号鍵ｋｆと個別暗号鍵ｋｅを使用して受信した認証データを更新し、通信制御部１７を介して中継装置３に返送する。

【００４４】通信制御部１７は、中継装置３との通信を制御する。

【００４５】図１に示す中継装置３は、店舗内に設置されている各読書装置１から決済金額情報を受信し、それらを集約（集計等）して、所定のタイミングで決済センタ５に送信する。また、中継装置３は、各読書装置１を認証するため、所定のタイミングで、店舗内の全ての読書装置１に共通に設定されているグローバルアドレスを指定して、全読書装置１に認証データを一斉に送信する。

【００４６】中継装置３は、図３に示すように、記憶部２１と、制御部２３と、通信制御部２５と、を備える。

【００４７】記憶部２１は、通信制御部２５を介して店舗内の各読書装置１から受信した決済金額情報を記憶する。また、記憶部２１は、複数の読書装置１に共通な共通暗号鍵ｋｆと各読書装置１に固有の個別暗号鍵ｋｅ（ｋｅ１、ｋｅ２、・・・、ｋｅｎ；ｎは読書装置１の数）を記憶する。共通暗号鍵ｋｆは、全ての読書装置１の記憶部１３に記憶されている共通暗号鍵ｋｆと同一の暗号鍵である。また、複数の個別暗号鍵ｋｅ（ｋｅ１、ｋｅ２、・・・、ｋｅｎ）は、各読書装置１の記憶部１３に記憶されている個別暗号鍵ｋｅにそれぞれ１対１に対応する（同一である）。

【００４８】また、記憶部２１は、各読書装置１を認証するために使用する図４（ａ）に示す検証データと、図４（ｂ）に示す検証用暗号データと、図４（ｃ）に示す認証データと、を記憶する。

【００４９】検証データは、図４（ａ）に示す様に、ｎ（ｎは読書装置の数）個のデータブロックを有する平文データから構成されている。検証用暗号データは、図４（ｂ）に示す様に、図４（ａ）の検証データをデータブロックごとに対応する個別暗号鍵ｋｅ（ｋｅ１、ｋｅ２、・・・、ｋｅｎ）を使用して暗号化したデータ（データ１’～データｎ’）から構成される。認証データは、図４（ｃ）に示す様に、図４（ａ）の検証データ全体を共通暗号鍵ｋｆを使用して暗号化したデータ（データ１”～データｎ”）から構成される。さらに、記憶部２１は、自らを識別する装置ＩＤを記憶する。

【００５０】制御部２３は、通信制御部２５を介して店舗内の各読書装置１から受信した決済金額情報を集計し、店舗単位の決済金額の合計を示す決済合計額情報を生成する。また、制御部２３は、所定のタイミングで店舗内の各読書装置１が、正しい下位装置であるか否かを判別するため、図４（ｃ）の認証データをグローバルアドレスを指定し、通信制御部２５を介して全読書装置１に一斉に送信する。さらに、制御部２３は、各読書装置１で更新され、返送された認証データを使用して送信元の読書装置１を認証する認証処理を行う。

【００５１】通信制御部２５は、読書装置１及び決済センタ５との間の通信を制御する。

【００５２】図１に示す決済センタ５は、各店舗の中継装置３から決済合計額情報を受信し、それらを集約（集計等）する。決済センタ５は、図５に示すように、記憶部３１と、制御部３３と、通信制御部３５と、を備える。

【００５３】記憶部３１は、通信制御部３５を介して各中継装置３から受信した決済合計額情報を記憶する。また、記憶部３１は、各中継装置３を識別するＩＤ情報

と、各中継装置３の下位装置となる各読書装置１を識別するＩＤ情報とを記憶する。

【００５４】制御部３３は、通信制御部３５を介して各中継装置３から受信した決済合計額情報を集計する。また、制御部３３は、中継装置３が下位装置である読書装置１を認証できない場合に送信する異常情報を通信制御部３５を介して受信し、受信した異常情報から該当する読書装置１を特定すると共に異常原因を特定する異常処理を行う。

【００５５】通信制御部３５は、中継装置３との通信を制御する。

【００５６】次に、本システムの動作について、中継装置３が読書装置１に対して行う認証処理の流れに沿って説明する。

【００５７】まず、中継装置３が店舗内の読書装置１に対して行う認証処理を、各読書装置１がその際行う認証データ更新処理と合わせて、図６及び図７のフローチャートを参照して説明する。中継装置３は、図示せぬタイマ装置から得られる所定のタイミング或いは決済センタ５からの要請に基づいて、図６に示す下位装置認証処理を開始する。まず、中継装置３は、通信制御部２５を介して、図４（ｃ）に示す認証データと認証処理の実行を指示する指示コマンドとを、読書装置１のグローバルアドレス（共通アドレス）を指定して各読書装置１に一斉に送信する（ステップＳ１）。

【００５８】認証データを受信した各読書装置１は、図７に示す認証データ更新処理を開始する。まず、制御部１５は、通信制御部１７を介して受信した認証データ（図４（ｃ））全体を、共通暗号鍵ｋｆを使用して復号化し、図８（ａ）に示す平文の認証データ（図４（ａ）に示す検証データに等しい）を生成する（ステップＳ１１）。

【００５９】次に、各読書装置１の制御部１５は、復号化した認証データのうちの、自己に割り付けられたデータブロックのデータを記憶部１３に記憶された個別暗号鍵ｋｅを使用して暗号化する（ステップＳ１２）。例えば、論理的に第ｉの読書装置１は、個別暗号鍵ｋｅｉを使用して、復号化された認証データ中の第ｉのデータブロックを、図８（ｂ）に示すように暗号化する。なお、ｉは、記憶部１３に記憶された装置ＩＤから特定される装置の論値的番号であり、１～ｎの整数である。

【００６０】次に、制御部１５は、図８（ｂ）に示すように第ｉのデータブロックだけが更新された認証データ全体を、図８（ｃ）に示すように、共通暗号鍵ｋｆを使用して暗号化する（ステップＳ１３）。なお、個別暗号鍵ｋｅｉで暗号化され、更に共通暗号鍵ｋｆで暗号化されたデータｉをデータｉ'''と表す。

【００６１】制御部１５は、図８（ｄ）に示すように、暗号化した更新済認証データに装置ＩＤ等を含むヘッダ情報を付加して、通信制御部１７を介して中継装置３に送信する（ステップＳ１４）。

【００６２】中継装置３は、図６に示すステップＳ２で、読書装置１で更新された認証データ（図９（ａ））を通信制御部２５を介して受信する。中継装置３は、受信したヘッダ情報と認証データとを分離し、分離した認証データを記憶部２１に記憶された共通暗号鍵ｋｆを使用して復号化する（ステップＳ３）。これにより、図９（ｂ）に示すように、第ｉのデータブロックだけが暗号鍵ｋｅｉで更新（暗号化）された検証データが生成される。

【００６３】次に、中継装置３は、ヘッダ情報に含まれている装置ＩＤから、更新されているデータブロックを判別し、図９（ｃ）及び（ｄ）に示すように、更新ブロック（データブロックｉ）と他の未更新データブロック（データブロック１～i-1、i+1～ｎ）とに分離する（ステップＳ４）。

【００６４】中継装置３は、記憶部２１に記憶されている図４（ａ）に示す検証データから、図９（ｂ）に示す未更新データブロックを抽出する。中継装置３は、検証データから抽出したデータと、図９（ｄ）に示す受信した未更新データブロックとが一致するか否かを判別する（ステップＳ５）。

【００６５】検証データから抽出したデータと受信した未更新データブロックとが一致しない場合は、認証対象の読書装置１が共通暗号鍵ｋｆを適切に使用して認証処理ができない異常な装置の場合である。従って、中継装置３は、通信制御部２５を介して、装置異常を示す異常コードと読書装置１を特定する装置ＩＤと、中継装置３を識別する装置ＩＤとからなる異常情報を決済センタ５に送信する（ステップＳ７）。

【００６６】一方、検証データから抽出したデータと受信した未更新データブロックとが一致すると判別された場合、中継装置３は、予め記憶部２１に記憶された図４（ｂ）に示す検証用暗号データから、受信した装置ＩＤで特定されるデータブロックと同一のデータブロック（データブロックｉ）を抽出する。中継装置３は、この抽出したデータブロックと、図９（ｃ）に示す更新データブロック（データブロックｉ）とが一致するか否かを判別する（ステップＳ６）。

【００６７】抽出したデータブロックと更新データブロックとが一致しない場合は、読書装置１自体は共通暗号鍵ｋｆでデータを処理できる装置、即ち、このシステムで使用できる装置であるが、装置ＩＤや暗号鍵ｋｅｉの設定が不適切なものと推定される。そこで、中継装置３は、設定異常を示す識別コードと、読書装置１を特定する装置ＩＤと、中継装置３を識別する装置ＩＤとからなる異常情報を決済センタ５に送信する（ステップＳ８）。

【００６８】一方、ステップＳ６で抽出したデータブロック（データブロックｉ）と更新データブロック（デー

タブロックｉ）とが一致すると判別された場合は、認証データを返送した読書装置１が、暗号鍵ｋｆとｋｅｉを適切に使用できるものであることから、中継装置３との間で個別に認証されたこととなり、中継装置３は、必要に応じて、任意の処理を開始する。

【００６９】次に、決済センタ５が中継装置３から異常情報を受信した場合の異常装置特定処理を、図１０のフローチャートを参照して説明する。

【００７０】中継装置３から異常情報を受信した決済センタ５は、図１０に示す異常処理を開始する。まず、制御部３３は、通信制御部１７を介して受信した異常情報から中継装置３を識別する装置ＩＤと読書装置１を識別する装置ＩＤとを抽出する。制御部３３は、抽出した２つの装置ＩＤから該当する読書装置１及びその店舗を特定する（ステップＳ２１）。

【００７１】次に、制御部３３は、受信した異常情報から異常識別コードを抽出し、抽出した異常識別コードが装置異常を示すか設定異常を示すかを判別する（ステップＳ２２）。

【００７２】制御部３３は、抽出した識別コードが装置異常（即ち、共通暗号鍵ｋｆによる認証エラー）を示す場合は、図示せぬ表示装置にステップＳ２１において特定した読書装置１及びその店舗を示す装置情報と、装置異常を示す異常メッセージとを表示し、管理者に通知する（ステップＳ２３）。装置異常が通知された管理者は、偽物装置による不当な売り上げを防止するため、例えば、該当する読書装置１の上位装置となる中継装置３から受信した決済情報の集計を停止する等の処置を取る。また、該当する読書装置１の回収等を保守作業者に連絡する。

【００７３】一方、制御部３３は、ステップＳ２２において、識別コードが装置異常を指示しているものではないと判別した場合に、抽出した識別コードが設定異常を示しているか否かを判別する（ステップＳ２４）。

【００７４】制御部３３は、抽出した識別コードが設定異常を示している場合に、図示せぬ表示装置に異常が検出された読書装置１及びその店舗を示す装置情報と、設定異常を示すメッセージとを表示し、管理者に通知する（ステップＳ２５）。設定異常は、読書装置１自体は、このプリペイドカードシステムで使用可能な正当な装置であるが、何らかの原因で、個別暗号鍵ｋｅｉが誤って設定されたり、装置の配置が誤っているなどの原因で発生すると推測される。そこで、読書装置１の設定異常を通知された管理者は、例えば、該当する読書装置１の再設定を保守作業者に連絡する。

【００７５】一方、制御部３３は、ステップＳ２４において、識別コードが設定異常を指示しているものではないと判別した場合に、予め設定された他の理由による不正データを受信したものと判別する。制御部３３は、図示せぬ表示装置にステップＳ２１において特定した読書装置１及びその店舗を示す装置情報と、不正データ受信を示す異常メッセージとを表示し、管理者に通知する（ステップＳ２６）。

【００７６】以上説明したように、この実施の形態では、中継装置３は、認証データを複数の読書装置１に一斉に送信し、各読書装置１から返送されて来た認証データを認証に使用する。このため、通信による読書装置１の認証を高速化することができる。また、二重に暗号化された認証データを認証に使用することにより、共通暗号鍵ｋｆで認証されなかった読書装置１を偽物装置の可能性が高いと推測し、個別暗号鍵ｋｅｉで認証できなかった読書装置１を誤って設定された装置であると推測することができる等、認証エラーの原因も推測することができる。

【００７７】上記の実施の形態では、中継装置３が各読書装置１に対してだけ認証処理を行ったが、さらに決済センタ５が各中継装置３に対して認証処理を行ってもよい。決済センタ５が各中継装置３に対する認証処理を行うことで、全体としてのセキュリティを向上させることができる。

【００７８】中継装置３が、読書装置１から受信した認証データが正当なものであるか否かを判別する手法は任意である。

【００７９】例えば、上記実施の形態では、第ｉの読書装置の共通暗号鍵ｋｆを用いた認証のために、データブロックｉ以外のデータブロックが検証データに一致しているか否かを判別している。しかし、読書装置の設置ミスの場合には、データブロックｉ以外のデータブロックが更新されて返送される場合があり、検証データと受信したデータブロックが完全には一致しないこともあり得る。このため、受信した認証データのうちのデータブロックｉ以外の殆どのブロック（例えば、全体のデータブロックの８０%）が検証ブロックに一致する場合には、両データが一致すると判別し、装置異常は存在しないと判断してもよい。

【００８０】例えば、中継センタ３は、第ｉの読書装置１から受信した認証データを共通暗号鍵ｋｆで復号化し、復号化された認証データのうちの第１～第i-1及び第i+1～第ｎのデータブロックが検証データ（期待値）と一致するか否かを判別することにより装置異常を検出し、第ｉのデータブロックを個別暗号鍵ｋｅｉで復号化し、復号化された第ｉのデータブロックと検証データの第ｉのデータブロック（期待値）が一致するか否かを判別することにより個別的な認証を行ってもよい。

【００８１】また、受信データの期待値を予め用意しておき、受信した認証データを復号することなく、認証を行ってもよい。例えば、中継センタ３は、第ｉの読書装置１から受信した認証データの期待値を予め用意しておき、受信した認証データの第１～第i-1及び第i+1～第ｎのデータブロックと期待値の対応部分が一致するか否か

を判別することにより、装置異常の有無を検出し、受信した認証データの第ｉのデータブロックと期待値の対応部分とを比較することにより、設定異常の有無を検証してもよい。この場合、受信データを復号化することなく、認証を行うことができ、認証を高速化できる。

【００８２】その他、この発明は、認証側の装置において、受信した認証対象のデータが共通暗号鍵及び個別暗号鍵により適切に処理（暗号化、復号化）されているか否かを判別することができるならば、判別手法は任意に選択可能である。

【００８３】なお、認証処理を実行するタイミングは、任意である。例えば、中継装置３の図示せぬ入力部から認証指示が入力されたタイミングで認証処理を開始してもよい。この構成により、読書装置１に使用する暗号鍵の変更作業や読書装置１の設置作業の完了時に、認証処理を実施し、作業の確認をすることができる。

【００８４】また、中継装置３が検証データを暗号化するために使用する共通暗号鍵と各読書装置１が更新済みの認証データを暗号化するために使用する共通暗号鍵は異なっていてもよい。また、共通暗号鍵を使用する方法に限定されず、複数の読書装置１に共通ならば、他の暗号方式を使用してもよい。

【００８５】さらに、各読書装置は、個別暗号鍵を互いに異ならせるだけでなく、暗号化方式自体を異ならせてもよい。

【００８６】中継装置３および読書装置１を構成するネットワーク形状は、任意である。例えば、リング型のネットワーク形状としてもよい。

【００８７】以上の実施の形態では、中継装置３が認証データのグローバルアドレスを指定し各読書装置１に一斉に送信しているが、通信プロトコル等の制約から１電文の最大長が決まっている場合は、複数回に分けて送信してもよい。例えば、ＨＤＬＣ手順の場合に、認証データの１データブロックを８バイトとすると、中継装置３は、１フレームで約３２台の読書装置１に認証データを送信することができる。このとき、読書装置１が３２台より多い場合には、中継装置３は、認証データを複数のフレームに分けて送信する。

【００８８】また、この発明は、プリペイドカードシステムに適用する場合に限定されず、ある管理装置が複数の管理対象装置を認証する場合に広く適用可能である。

【００８９】

【発明の効果】以上説明したように、本発明によれば、認証装置から認証対象装置に認証データを一斉に送信することにより、認証処理を高速化することができる。また、認証データ全体の暗号化と一部分のデータの暗号化とを組み合わせて使用することにより、認証対象装置の認証ミスの原因を判別することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るプリペイドカードシステムの構成を示す図である。

【図２】読書装置１の構成を示す図である。

【図３】中継装置３の構成を示す図である。

【図４】検証データ、検証用暗号データ及び認証データを示す図である。

【図５】決済センタ５の構成を示す図である。

【図６】上位装置が行う認証処理のフローチャートである。

【図７】下位装置が行う認証データ更新処理のフローチャートである。

【図８】下位装置で更新（暗号化）される認証データを示す図である。

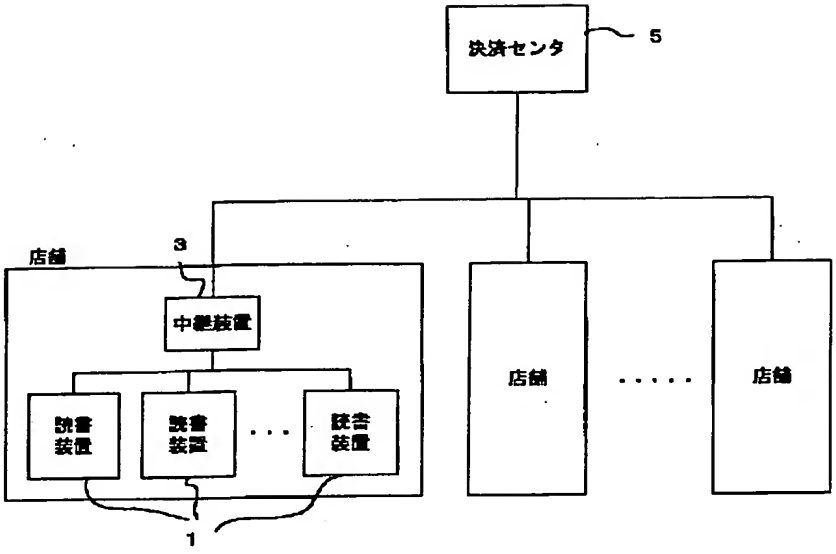
【図９】上位装置で認証（データ分離等）される認証データを示す図である。

【図１０】上位装置が行う異常装置特定処理のフローチャートである。

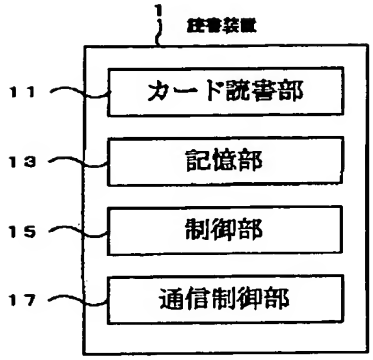
【符号の説明】

１　読書装置
３　中継装置
５　決済センタ
１１　カード記録部
１３　記憶部
１５　制御部
１７　通信制御部
２１　記憶部
２３　制御部
２５　通信制御部
３１　記憶部
３３　制御部
３５　通信制御部

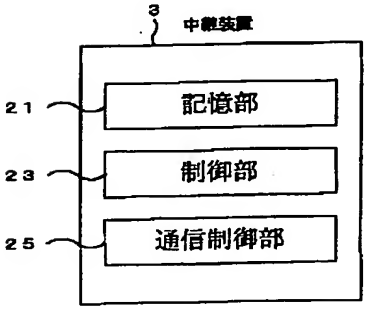
【図１】


決済センタ
5
店舗
3
中継装置
読書装置
読書装置
読書装置
1
店舗
店舗

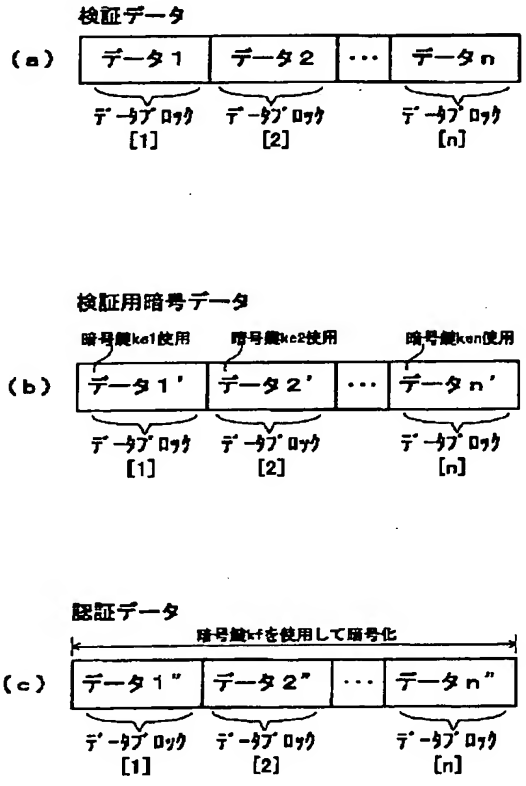
【図２】


1
読書装置
11
カード読書部
13
記憶部
15
制御部
17
通信制御部

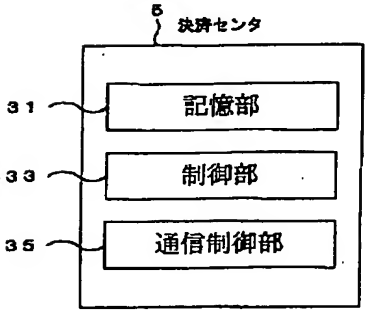
【図３】


3
中継装置
21
記憶部
23
制御部
25
通信制御部

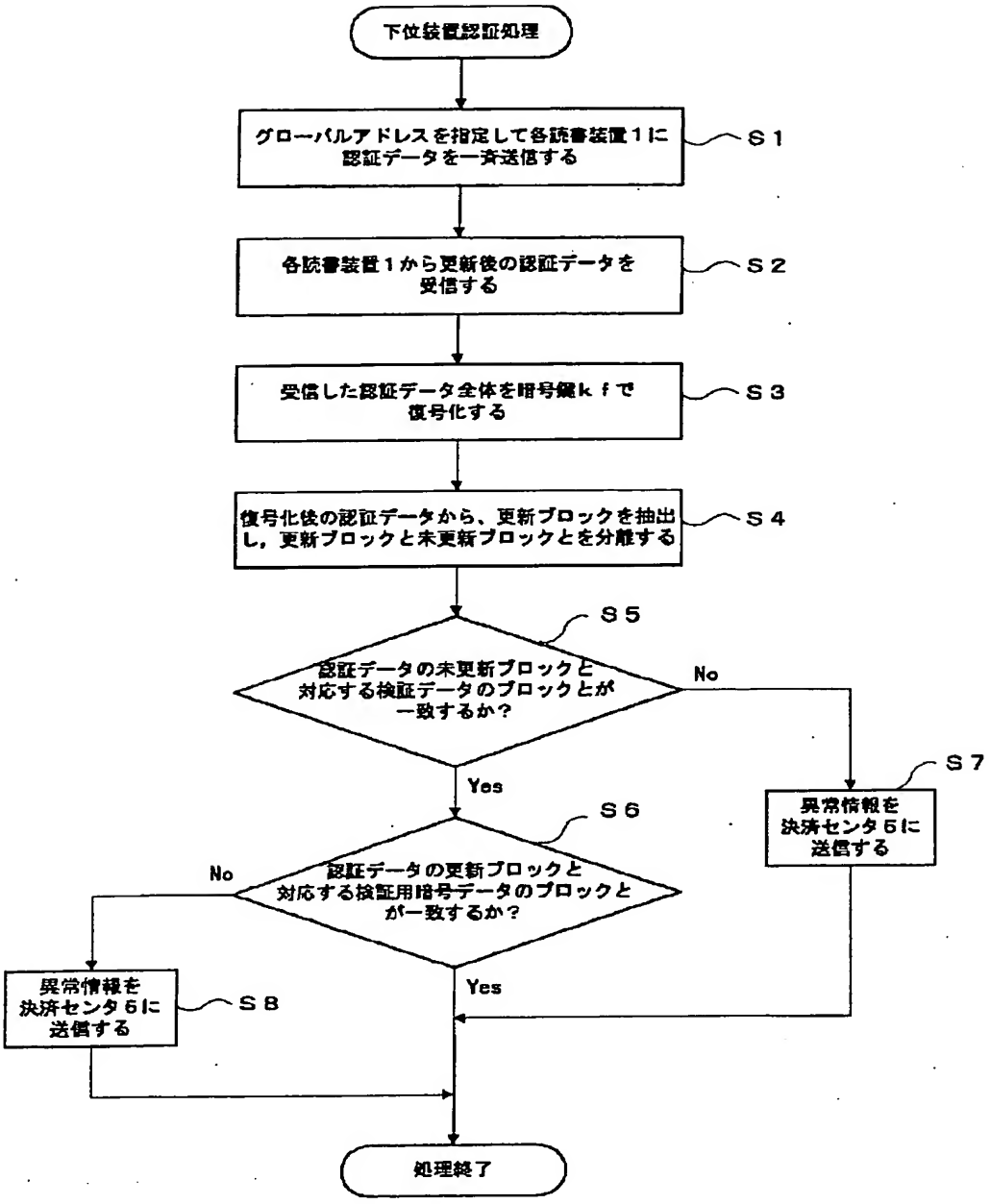
【図４】


検証データ
(a)
データ１
データ２
・・・
データｎ
データブロック [1]
データブロック [2]
データブロック [n]
検証用暗号データ
暗号鍵ke1使用
暗号鍵ke2使用
暗号鍵ken使用
(b)
データ１'
データ２'
・・・
データｎ'
データブロック [1]
データブロック [2]
データブロック [n]
認証データ
暗号鍵kfを使用して暗号化
(c)
データ１"
データ２"
・・・
データｎ"
データブロック [1]
データブロック [2]
データブロック [n]

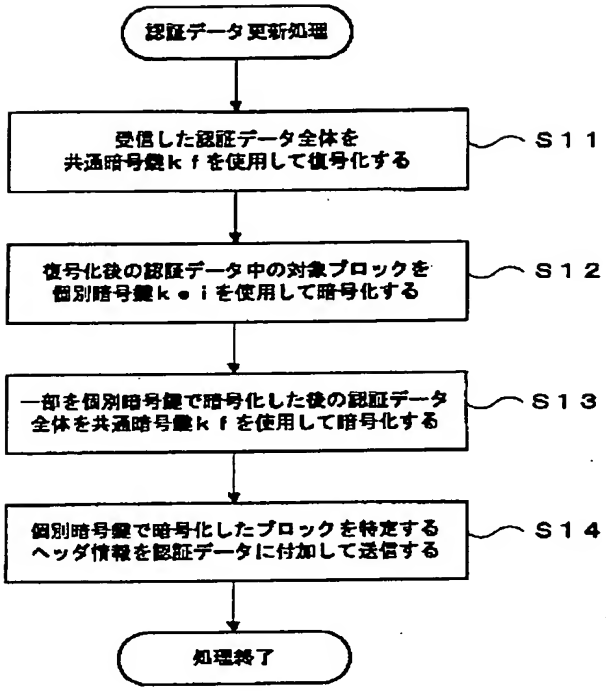
【図５】


5
決済センタ
31
記憶部
33
制御部
35
通信制御部

【図６】

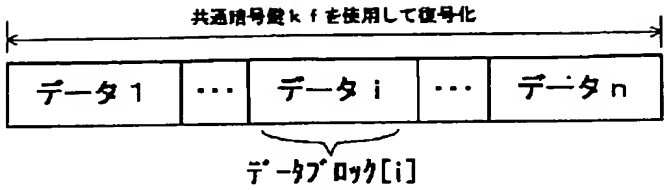

下位装置認証処理
グローバルアドレスを指定して各読書装置１に認証データを一斉送信する
Ｓ１
各読書装置１から更新後の認証データを受信する
Ｓ２
受信した認証データ全体を暗号鍵ｋｆで復号化する
Ｓ３
復号化後の認証データから、更新ブロックを抽出し，更新ブロックと未更新ブロックとを分離する
Ｓ４
Ｓ５
認証データの未更新ブロックと対応する検証データのブロックとが一致するか？
No
Yes
Ｓ７
異常情報を決済センタ５に送信する
Ｓ６
認証データの更新ブロックと対応する検証用暗号データのブロックとが一致するか？
No
Yes
異常情報を決済センタ６に送信する
Ｓ８
処理終了

【図７】

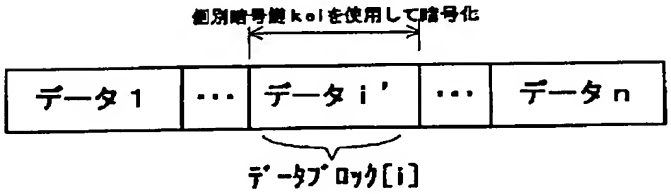

認証データ更新処理
受信した認証データ全体を
共通暗号鍵ｋｆを使用して復号化する
Ｓ１１
復号化後の認証データ中の対象ブロックを
個別暗号鍵ｋｏｉを使用して暗号化する
Ｓ１２
一部を個別暗号鍵で暗号化した後の認証データ
全体を共通暗号鍵ｋｆを使用して暗号化する
Ｓ１３
個別暗号鍵で暗号化したブロックを特定する
ヘッダ情報を認証データに付加して送信する
Ｓ１４
処理終了

【図８】

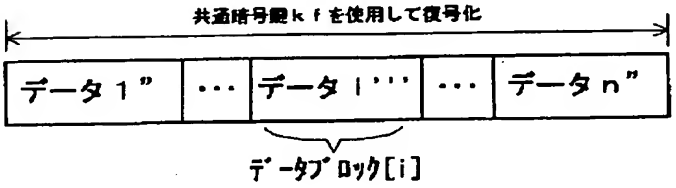
(a)


共通暗号鍵ｋｆを使用して復号化
データ１
・・・
データｉ
・・・
データｎ
データブロック[i]

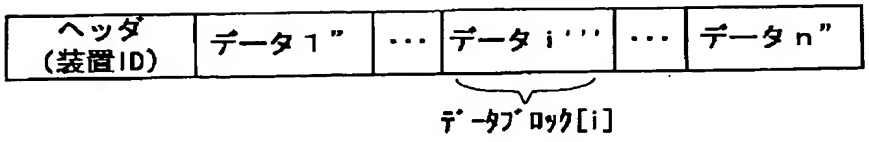
(b)


個別暗号鍵ｋｏｉを使用して暗号化
データ１
・・・
データｉ’
・・・
データｎ
データブロック[i]

(c)

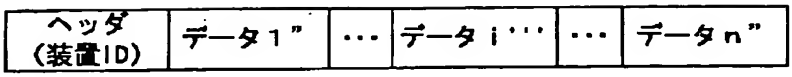

共通暗号鍵ｋｆを使用して復号化
データ１”
・・・
データｉ’’’
・・・
データｎ”
データブロック[i]

(d)

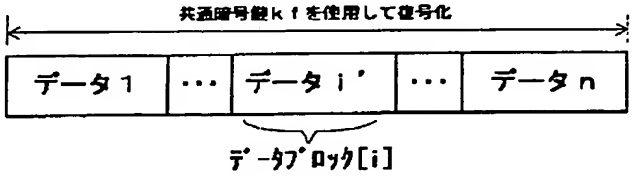

ヘッダ
(装置ID)
データ１”
・・・
データｉ’’’
・・・
データｎ”
データブロック[i]

【図９】

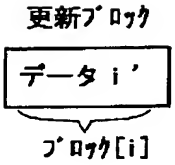
(a)


ヘッダ
(装置ID)
データ１”
・・・
データｉ’・・・
・・・
データｎ”

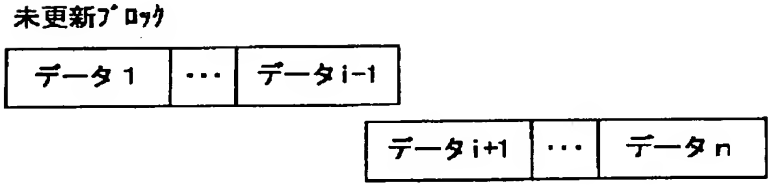
(b)


共通暗号鍵ｋｆを使用して復号化
データ１
・・・
データｉ’
・・・
データｎ
ﾃﾞｰﾀﾌﾞﾛｯｸ[i]

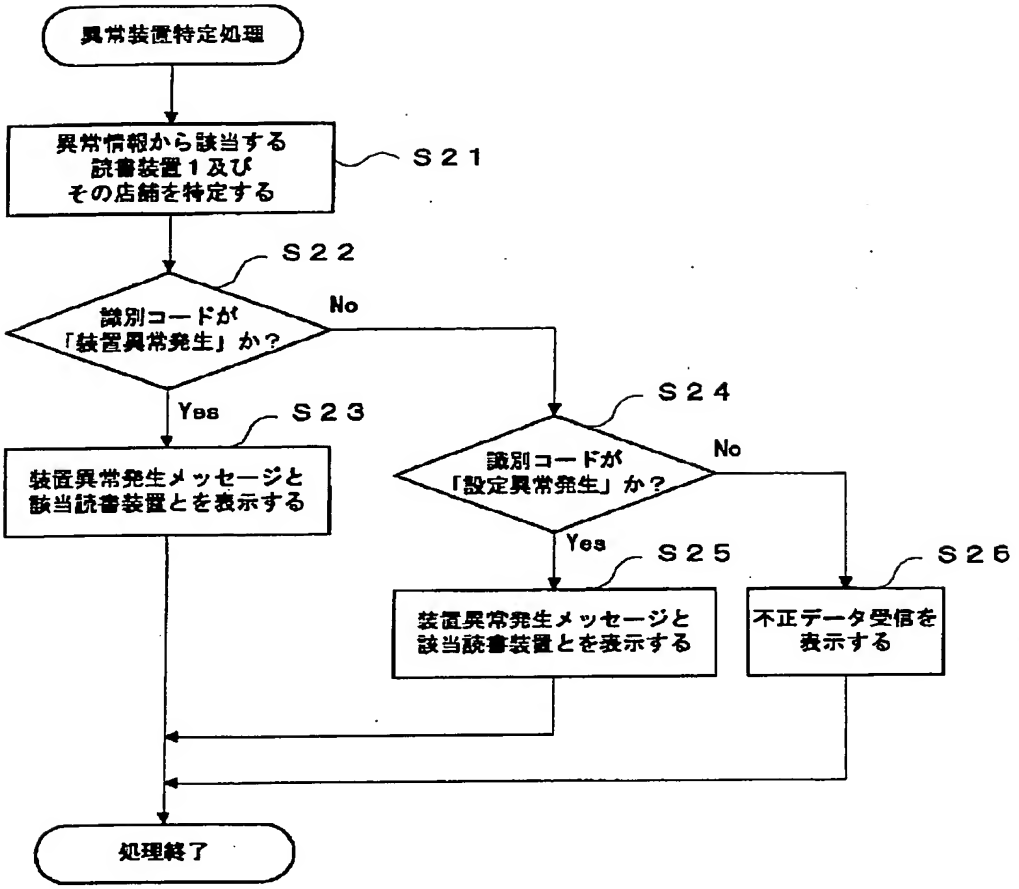
(c)


更新ﾌﾞﾛｯｸ
データｉ’
ﾌﾞﾛｯｸ[i]

(d)


未更新ﾌﾞﾛｯｸ
データ１
・・・
データi-1
データi+1
・・・
データｎ

【図１０】



フロントページの続き

(51) Int. Cl. 6	識別記号	ＦＩ
		Ｇ０７Ｆ　7/08　Ｌ